(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10271106 A

(43) Date of publication of application: 09.10.98

(51) Int. Cl H04L 9/10
H04L 9/08

(21) Application number: 09068460

(22) Date of filing: 21.03.97

(71) Applicant: NIPPON TELEGR & TELEPH CORP <NTT>

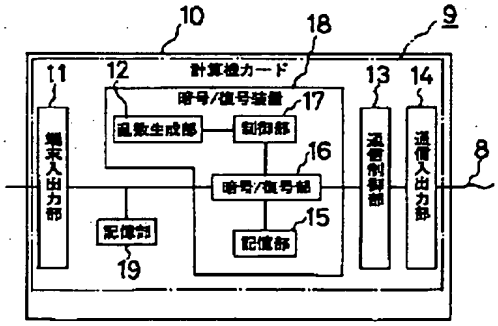
(72) Inventor: TAKADA SHUNSUKE
KAWAKUBO HIDEJI

(54) CIPHER COMMUNICATION METHOD AND SYSTEM EQUIPMENT

(57) Abstract:

PROBLEM TO BE SOLVED: To perform the cipher communication of high safety by packaging and loading a secrecy protected ciphering/deciphering device to a computer card incorporated in a communication controller for connecting an information terminal equipment to a communication path and performing ciphering/ deciphering processings together for the transfer of the input/output of secret data between the information terminal equipment and the communication path.

SOLUTION: Through the terminal and communication input/output parts 11 and 14 and communication control part 13 of a cipher communication equipment 9 packaged to the computer card 10 and by the control, the information terminal equipments are connected by the communication path 8. A random number generation part 12 generates a random number and generates a cipher key, a storage part 15 stores the secret key and program of a transmission side for ciphering/deciphering and the storage part 19 stores the public key of a reception opposite side. A ciphering/deciphering part 16 executes the processing of ciphering/deciphering by using the cipher key and the public key by the control of a control part 17 and the ciphering/deciphering device 18 physically protects the secrecy of the respective parts inside. Thus, without uselessly consuming hardware resources, safe communication is made possible.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－271106

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ
9/08			６０１Ａ

審査請求　未請求　請求項の数19　ＯＬ　（全８頁）

(21)出願番号　特願平9－68460

(22)出願日　平成９年(1997)３月21日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　高田　俊介
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　河久保　秀二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

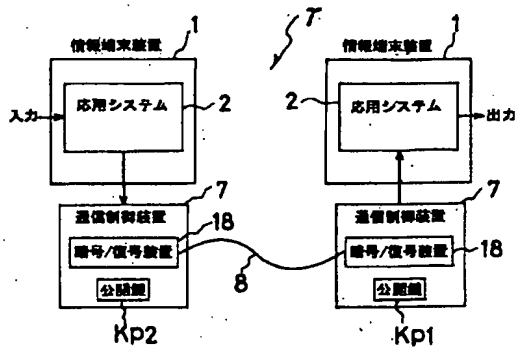
(74)代理人　弁理士　菅　隆彦

(54)【発明の名称】　暗号通信方法及びシステム装置

(57)【要約】

【課題】安全性が高く情報端末装置のハードウェアリソースを有効に利用出来る暗号通信方法及びシステム装置の提供。

【解決手段】情報端末装置１を通信路８に接続する通信制御装置７に内蔵され、乱数生成部１２と記憶部１５と暗号／復号部１６と制御部１７とを備える暗号／復号装置１８を搭載した暗号通信システム装置γの特徴。



1

【特許請求の範囲】

【請求項１】送信側で、
情報端末手段から受信したデータを機密が保護された手段内で生成した暗号鍵で暗号化した後、
公開鍵暗号方式の受信側の公開鍵で当該暗号鍵を暗号化した保護暗号鍵と先に暗号化された前記データを通信路に送信し、
受信側で、
当該通信路から受信した暗号化された前記保護暗号鍵を前記公開鍵と対応付けた受信側の秘密鍵で復号して送信側の前記暗号鍵を抽出した後、
当該暗号鍵で受信した前記暗号化データを復号する、
ことを特徴とする暗号通信方法。

【請求項２】機密保護手段は、
情報端末手段を通信路に接続する通信制御手段に内設する、
ことを特徴とする請求項１に記載の暗号通信方法。

【請求項３】機密保護手段は、
計算機カード内に実装搭載する、
ことを特徴とする請求項１又は２に記載の暗号通信方法。

【請求項４】通信路は、
電話回線、ＩＳＤＮ、ＬＡＮ、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである、
ことを特徴とする請求項１、２又は３に記載の暗号通信方法。

【請求項５】送受信両側は、
当該両側で通信制御手段の計算機カード内に自己の公開鍵とこれに対応付けた秘密鍵を格納するステップ１と、
送受信側を接続するステップ２と、
送信者の公開鍵情報を受信側に送信して受信側で送信者の公開鍵情報を蓄積するステップ３と、
受信者の公開鍵情報を送信側に送信して送信側で受信者の公開鍵情報を蓄積するステップ４と、
の前処理段階を順次踏む、
ことを特徴とする請求項１又は４に記載の暗号通信方法。

【請求項６】通信路への送信は、
パケット通信である、
ことを特徴とする請求項１、２、３、４又は５に記載の暗号通信方法。

【請求項７】保護暗号鍵は、
パケットのヘッダに添付して送信する、
ことを特徴とする請求項１、２、３、４、５又は６に記載の暗号通信方法。

【請求項８】送信側は、
暗号化したデータと保護暗号鍵をパケット通信後、
受信側の復号処理の出力完了まで送信及び受信を一時待機し、
受信側と相互交信のないことを確認した上で送信終了する、
後処理段階を順次踏む、
ことを特徴とする請求項１、２、３、４、５、６又は７に記載の暗号通信方法。

2

【請求項９】受信側は、
復号したデータを端末に出力した後、
送信側からの追加受信の余裕時間まで送信及び受信を一時待機し、
送信側と相互交信のないことを確認した上で通信終了する、
後処理段階を順次踏む、
ことを特徴とする請求項１、２、３、４、５、６、７又は８に記載の暗号通信方法。

【請求項１０】通信路は、
インターネット、イントラネット、エキストラネット、ＯＣＮ、ＯＤＮ、仮想専用網、各種交換機網、ＶＡＮ等に接続又は利用した暗号データ伝送路を形成する、
ことを特徴とする請求項１、２、３、４、５、６、７、８又は９に記載の暗号通信方法。

【請求項１１】情報端末装置を通信路に接続する通信制御装置に内蔵され、
暗号／復号装置を搭載した、
ことを特徴とする暗号通信システム装置。

【請求項１２】暗号／復号装置は、
機密を保護された装置である、
ことを特徴とする請求項１１に記載の暗号通信システム装置。

【請求項１３】暗号／復号装置は、
情報端末装置との入出力を制御する端末入出力部と、
受信相手側の公開鍵情報を格納する記憶部と、
通信路との入出力を制御する通信制御部と、
実際に通信路との入出力を行う通信入出力部と、共に、
前記情報端末装置を前記通信路に接続する通信制御装置に内蔵する計算機カード上に一体に実装搭載する、
ことを特徴とする請求項１１又は１２に記載の暗号通信システム装置。

【請求項１４】暗号／復号装置は、
暗号鍵を作成するための乱数を生成する乱数生成部と、
復号のための自己の秘密鍵やプログラムを蓄積する記憶部と、
前記暗号鍵を使用してデータの暗号／復号を行う暗号／復号部と、
暗号／復号の処理を制御する制御部と、を備える、
ことを特徴とする請求項１１、１２又は１３に記載の暗号通信システム装置。

【請求項１５】通信路は、
電話回線、ＩＳＤＮ、ＬＡＮ、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである、
ことを特徴とする請求項１１、１２、１３又は１４に記載の暗号通信システム装置。

【請求項１６】通信路は、
インターネット、イントラネット、エキストラネット、ＯＣＮ、ＯＤＮ、仮想専用網、各種交換機網、ＶＡＮ等に接続又は利用した暗号データ伝送路を形成する、
ことを特徴とする請求項１１、１２、１３、１４又は１５に記載の暗号通信システム装置。
【請求項１７】情報端末装置は、
パソコン、ワークステーション、インテリジェント端末、電話器、ＦＡＸ、交換機、電子メール端末、無線機、移動通信端末等を含む、
ことを特徴とする請求項１１、１２、１３、１４、１５又は１６に記載の暗号通信システム装置。
【請求項１８】受信相手側の公開鍵情報を格納する記憶部は、
暗号／復号装置内の復号のための自己の秘密鍵やプログラムを蓄積する記憶部と兼用する、
ことを特徴とする請求項１３、１４、１５、１６又は１７に記載の暗号通信システム装置。
【請求項１９】受信相手側の公開鍵情報を格納する記憶部は、
暗号／復号装置内に復号のための自己の秘密鍵やプログラムを蓄積する記憶部と別に並設する、
ことを特徴とする請求項１３、１４、１５、１６又は１７に記載の暗号通信システム装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報端末装置を通して各種暗号データを相互交信するのに供される暗号通信方法及びその実施に直接使用するシステム装置に関する。
【０００２】
【従来の技術】近年、オープンなネットワーク及びイントラネット等におけるリモートアクセスにおいて、情報の盗聴、改ざん、なりすましの脅威に対処する方法が検討されている。
【０００３】従来、ネットワークで通信される情報を保護する方法において、図５に示すように情報端末装置１内の応用システム２に暗号／復号装置３と暗号鍵４を保持するシステム装置αや、図６に示すように計算機カードなどの外部記憶装置５内に暗号鍵６を保持するシステム装置βが知られている。なお、図中、７は通信制御装置、８は通信路である。
【０００４】
【発明が解決しようとする課題】前述した従来の暗号方法において、図５の方法は秘密情報である暗号鍵４を情報端末装置１内に保持しその暗号鍵４を使用してメッセージを暗号化するシステム装置αを用いた手法である。この場合、通常暗号鍵４は秘密鍵などで暗号化して格納するが、実際に暗号処理を行う際に使用する暗号鍵４が復号されてメインメモリ上に展開されるため、盗聴される危険があり、また暗号鍵４の盗難や消去される危険がある。
【０００５】図６の方法では、暗号鍵６を外部記憶装置５に保持し、情報端末装置１で暗号／復号処理を行う際に暗号鍵６を読み出して処理するシステム装置βを用いた手法である。この場合、暗号鍵６の盗難や消去に対する安全性は向上するが、処理実行中に暗号鍵６がメインメモリ上に展開される問題が解決できない。また、外部記憶装置５と通信制御装置７を同時に使用するため、情報端末装置１のハードウェアリソースの競合の問題も生ずる。
【０００６】ここにおいて、本発明の解決すべき主要な目的は、次の通りである。本発明の第１の目的は、上記の問題を解決し、安全性が高く情報端末装置のハードウェアリソースを有効に利用できる暗号通信方法及びシステム装置を提供せんとするものである。
【０００７】本発明の第２の目的は、通信制御装置内に暗号／復号装置を組み込んで暗号／復号処理を行う暗号通信方法及びシステム装置を提供せんとするものである。
【０００８】本発明の第３の目的は、暗号鍵と秘密鍵と保護暗号鍵の三重鍵を駆使した暗号通信方法及びシステム装置を提供せんとするものである。
【０００９】本発明の第４の目的は、暗号／復号装置を通信制御装置内に装備した計算機カードに秘密が保護されて実装搭載する暗号通信方法及びシステム装置を提供せんとするものである。
【００１０】本発明のその他の目的は、明細書及び図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。
【００１１】
【課題を解決するための手段】本発明は、前記課題を解決するのに当り、情報端末装置を通信路に接続する通信制御装置に内蔵した計算機カードに秘密が保護された暗号／復号装置を実装搭載し、前記情報端末装置と前記通信路間の秘密データの入出力のやり取りに際し、暗号／復号処理を併せ行う。
【００１２】その際、前記暗号／復号装置内で作成した暗号鍵でデータを暗号化するとともに当該暗号鍵を公開鍵暗号方式の受信側の公開鍵で暗号化した保護暗号鍵を前記暗号化データと一緒に受信側に送信する。受信側では当該保護暗号鍵から前記公開鍵と対応付けた受信側の秘密鍵で暗号鍵を抽出し、その暗号鍵で暗号化データを復号処理する、所謂三重鍵をキーワードとして暗号解読のセキュリティを万全なものとしてある。特に電子マネーの授受に最適である。
【００１３】さらに、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙するそれぞれの新規な特徴的構成手法又は手段を採用することにより前記目的を達成する。

【００１４】即ち、本発明方法の第１の特徴は、送信側で、情報端末手段から受信したデータを機密が保護された手段内で生成した暗号鍵で暗号化した後、公開鍵暗号方式の受信側の公開鍵で当該暗号鍵を暗号化した保護暗号鍵と先に暗号化された前記データを通信路に送信し、受信側で、当該通信路から受信した暗号化された前記保護暗号鍵を前記公開鍵と対応付けた受信側の秘密鍵で復号して送信側の前記暗号鍵を抽出した後、当該暗号鍵で受信した前記暗号化データを復号してなる暗号通信方法の構成採用にある。

【００１５】本発明方法の第２の特徴は、前記本発明方法の第１の特徴における機密保護手段が、情報端末手段を通信路に接続する通信制御手段に内設してなる暗号通信方法の構成採用にある。

【００１６】本発明方法の第３の特徴は、前記本発明方法の第１又は第２の特徴における機密保護手段が、計算機カード内に実装搭載してなる暗号通信方法の構成採用にある。

【００１７】本発明方法の第４の特徴は、前記本発明方法の第１、第２又は第３の特徴における通信路が、電話回線、ＩＳＤＮ、ＬＡＮ、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである暗号通信方法の構成採用にある。

【００１８】本発明方法の第５の特徴は、前記本発明方法の第１又は第４の特徴における送受信両側が、当該両側で通信制御手段の計算機カード内に自己の公開鍵とこれに対応付けた秘密鍵を格納するステップ１と、送受信側を接続するステップ２と、送信者の公開鍵情報を受信側に送信して受信側で送信者の公開鍵情報を蓄積するステップ３と、受信者の公開鍵情報を送信側に送信して送信側で受信者の公開鍵情報を蓄積するステップ４と、の前処理段階を順次踏んでなる暗号通信方法の構成採用にある。

【００１９】本発明方法の第６の特徴は、前記本発明方法の第１、第２、第３、第４又は第５の特徴における通信路への送信が、パケット通信である暗号通信方法の構成採用にある。

【００２０】本発明方法の第７の特徴は、前記本発明方法の第１、第２、第３、第４、第５又は第６の特徴における保護暗号鍵が、パケットのヘッダに添付して送信してなる暗号通信方法の構成採用にある。

【００２１】本発明方法の第８の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６又は第７の特徴における送信側が、暗号化したデータと保護暗号鍵をパケット通信後、受信側の復号処理の出力完了まで送信及び受信を一時待機し、受信側と相互交信のないことを確認した上で送信終了する、後処理段階を順次踏んでなる暗号通信方法の構成採用にある。

【００２２】本発明方法の第９の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６、第７又は第８の特徴における受信側が、復号したデータを端末に出力した後、送信側からの追加受信の余裕時間まで送信及び受信を一時待機し、送信側と相互交信のないことを確認した上で通信終了する、後処理段階を順次踏んでなる暗号通信方法の構成採用にある。

【００２３】本発明方法の第１０の特徴は、前記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８又は第９の特徴における通信路が、インターネット、イントラネット、エキストラネット、ＯＣＮ、ＯＤＮ、仮想専用網、各種交換機網、ＶＡＮ等に接続又は利用した暗号データ伝送路を形成してなる暗号通信方法の構成採用にある。

【００２４】本発明装置の第１の特徴は、情報端末装置を通信路に接続する通信制御装置に内蔵され、暗号／復号装置を搭載した暗号通信システム装置の構成採用にある。

【００２５】本発明装置の第２の特徴は、前記発明装置の第１の特徴における暗号／復号装置が、機密を保護された装置である暗号通信システム装置の構成採用にある。

【００２６】本発明装置の第３の特徴は、前記本発明装置の第１又は第２の特徴における暗号／復号装置が、情報端末装置との入出力を制御する端末入出力部と、受信相手側の公開鍵情報を格納する記憶部と、通信路との入出力を制御する通信制御部と、実際に通信路との入出力を行う通信入出力部と、共に、前記情報端末装置を前記通信路に接続する通信制御装置に内蔵する計算機カード上に一体に実装搭載してなる暗号通信システム装置の構成採用にある。

【００２７】本発明装置の第４の特徴は、前記発明装置の第１、第２又は第３の特徴における暗号／復号装置が、暗号鍵を作成するための乱数を生成する乱数生成部と、復号のための自己の秘密鍵やプログラムを蓄積する記憶部と、前記暗号鍵を使用してデータの暗号／復号を行う暗号／復号部と、暗号／復号の処理を制御する制御部と、を備えてなる暗号通信システム装置の構成採用にある。

【００２８】本発明装置の第５の特徴は、前記本発明装置の第１、第２、第３又は第４の特徴における通信路が、電話回線、ＩＳＤＮ、ＬＡＮ、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである暗号通信システム装置の構成採用にある。

【００２９】本発明装置の第６の特徴は、前記本発明装置の第１、第２、第３、第４又は第５の特徴における通信路が、インターネット、イントラネット、エキストラネット、ＯＣＮ、ＯＤＮ、仮想専用網、各種交換機網、ＶＡＮ等に接続又は利用した暗号データ伝送路を形成してなる暗号通信システム装置の構成採用にある。

【００３０】本発明装置の第７の特徴は、前記本発明装置の第１、第２、第３、第４、第５又は第６の特徴にお

ける情報端末装置が、パソコン、ワークステーション、インテリジェント端末、電話器、ＦＡＸ、交換機、電子メール端末、無線機、移動通信端末等を含んでなる暗号通信システム装置の構成採用にある。

【００３１】本発明装置の第８の特徴は、前記本発明装置の第３、第４、第５、第６又は第７の特徴における受信相手側の公開鍵情報を格納する記憶部が、暗号／復号装置内の復号のための自己の秘密鍵やプログラムを蓄積する記憶部と兼用してなる暗号通信システム装置の構成採用にある。

【００３２】本発明装置の第９の特徴は、前記本発明装置の第３、第４、第５、第６又は第７の特徴における受信相手側の公開鍵情報を格納する記憶部が、暗号／復号装置内に復号のための自己の秘密鍵やプログラムを蓄積する記憶部と別に並設してなる暗号通信システム装置の構成採用にある。

【００３３】

【発明の実施の形態】本発明の実施の形態をその装置例及び方法例につき図面を参照して説明する。なお、本実施形態では、情報端末手段である情報端末装置はパソコン、ワークステーション、インテリジェント端末、電話器、ＦＡＸ、交換機、電子メール端末、無線機、移動通信端末等を含み、通信路には電話回線、ＩＳＤＮ、ＬＡＮ、無線、光通信、衛星通信等のいずれか又はこれ等の組合せで構成され、インターネット、イントラネット、エキストラネット、ＯＣＮ、ＯＤＮ、仮想専用網、各種交換機網、ＶＡＮ等に接続又は利用した暗号データ伝送路を形成する。

【００３４】（装置例）図１は本装置例を組み込んだ暗号通信システム装置の構成ブロック図、図２は本装置例の構成ブロック図である。なお、図５乃至図６に示す従来例の暗号通信システム装置α，βと同一装置及び部は同一符号を付して説明の重複を避けた。

【００３５】図中、γは本装置例を装備した暗号通信システム装置、９は本装置例の暗号通信装置、１０は暗号通信装置９を実装搭載する計算機カードの本体、１１は情報端末装置１と計算機カード１０の暗号通信装置９との入出力を制御する端末入出力部、１２は暗号鍵Ｋｅ１又はＫｅ２を作成するための乱数を生成する乱数生成部、１３は通信路８との入出力を制御する通信制御部、１４は実際に通信路８との入出力を行う通信入出力部である。

【００３６】１５は暗号／復号のための送信自己側の秘密鍵やプログラムを蓄積する記憶部、１６は前記暗号鍵Ｋｅ１又はＫｅ２や前記公開鍵Ｋｐ１又はＫｐ２や秘密鍵（図示せず）を使用して実際に暗号／復号を行う暗号／復号部、１７は暗号／復号の処理を制御する制御部、１８は乱数生成部１２と記憶部１５と暗号／復号部１６と制御部１７の機密を物理的に保護する暗号／復号装置、１９は受信相手側の公開鍵Ｋｐ２情報などを格納する記憶部である。なお、記憶部１９を記憶部１５と兼用しても良いし、記憶部１９を暗号／復号装置１８内に記憶部１５と並存しても一向に構わない。

【００３７】（方法例）当該本装置例に適用する本方法例の実行手順を図面について説明する。図３は本方法例の暗号通信処理手順を示すフローチャート、図４は同・シーケンスチャートである。

【００３８】（１）通信前処理段階Ｘ

まず、本方法例で使用する計算機カード１０発行時にそのカード１０の秘密情報である公開鍵暗号方式の自己の公開鍵Ｋｐ１（Ｋｐ２）に対応付けた図示しない秘密鍵を記憶部１５に、公開鍵Ｋｐ１（Ｋｐ２）を記憶部１９にそれぞれ格納し（ＳＴ１）、相手側の公開鍵Ｋｐ２（Ｋｐ１）を記憶部１９に格納する。

【００３９】利用者Ａと利用者Ｂは、電話回線、ＩＳＤＮ、ＬＡＮ、無線、光通信、衛星通信等においてそれぞれ通常行われる接続要求情報Ｓ１と接続許可情報Ｓ２との交信手順により相互接続を確立し（ＳＴ２）、利用者Ａが使用する計算機カード１０の公開鍵情報Ｋｐ１と利用者Ｂが使用する計算機カード１０の公開鍵情報Ｋｐ２をそれぞれ交換して蓄積する（ＳＴ３，ＳＴ４）。

【００４０】（２）暗号／復号交信処理段階Ｙ

利用者Ａの送信側では、送信処理は、情報端末装置１からの送信データＭ１を端末入出力部１１で受信し（ＳＴ５）、送信データＭ１と受信側の公開鍵Ｋｐ２を物理的に機密が保護された暗号／復号装置１８に送る。暗号／復号装置１８では、まず制御部１７が乱数生成部１２で生成した乱数により暗号鍵Ｋｅ１を生成する（ＳＴ６）。

【００４１】次に、記憶部１５に格納されている暗号プログラムを呼び出し、暗号鍵Ｋｅ１を使用して暗号／復号部１６で送信データＭ１を暗号化する（ＳＴ７）。さらに制御部１７は記憶部１５に格納されている公開鍵暗号プログラムを呼び出し、受信側の公開鍵Ｋｐ２を使用して暗号／復号部１６で暗号鍵Ｋｅ１を暗号化する（ＳＴ８）。その上、通信御御部１３は、暗号化した送信データＫｅ１［Ｍ１］にヘッダ情報として暗号化した保護暗号鍵Ｋｐ２［Ｋｅ１］を付加したデータＫｅ１［Ｍ１］を受取り、通信入出力部１４から通信路８に送出する（ＳＴ１０）。

【００４２】他方、利用者Ｂの受信側では、受信側の計算機カード１０上の通信制御部１３が通信入出力部１４で通信路８からのデータＫｐ２［Ｋｅ１］・Ｋｅ１［Ｍ１］を受信し（ＳＴ６′）、暗号／復号装置１８に送る。暗号／復号装置１８では、制御部１７が受信データＫｐ２［Ｋｅ１］・Ｋｅ１［Ｍ１］から保護暗号鍵Ｋｐ２［Ｋｅ１］を抽出して（ＳＴ７′）、記憶部１５に格納されている公開鍵暗号プログラムと自分の公開鍵Ｋｐ２に対応付けた図示しない秘密鍵を呼び出し、自分の秘密鍵で保護暗号鍵Ｋｐ２［Ｋｅ１］を暗号鍵Ｋｅ１に復

号する（ＳＴ８′）。

【００４３】さらに制御部１７は、記憶部１５から復号プログラムを呼び出し暗号鍵Ｋｅ１で暗号化された送信データＫｅ１［Ｍ１］を復号し受信データＭ１を抽出する（ＳＴ９′）。最後に抽出した受信データＭ１を端末入出力部１１から情報端末装置１に出力する（ＳＴ１０′）。

【００４４】（３）後処理段階Ｚ

利用者Ａの送信側では、受信側の通信制御装置７で最終復号処理した受信データＭ１を情報端末装置１に出力完了するまで送信及び受信を一時待機し（ＳＴ１１）、その後受信側と相互交信のないことを確認した上で通信終了する（ＳＴ１２）。又、利用者Ｂの受信側では、送信側からの追加受信の余裕時間まで送信及び受信を一時待機し（ＳＴ１１′）、送信側と相互交信のないことを確認した上で通信終了する（ＳＴ１２′）。

【００４５】

【発明の効果】以上述べたように本発明によれば、計算機カード内に電話回線、ＩＳＤＮ、ＬＡＮ、無線、光通信などの通信装置と暗号／復号装置を持ち、また鍵の生成から暗号／復号処理までを機密が保護された装置内でのみ行うことにより、通信プログラムなどの応用システムに影響をおよぼさず、ハードウェアリソースを浪費することなく、安全な通信を実現できる。

【図面の簡単な説明】

【図１】本発明の実施形態を示す装置例を組み込んだ暗号通信システム装置の構成ブロック図である。

【図２】同上装置例の構成ブロック図である。

【図３】本発明の実施の形態を示す方法例の暗号通信処理手順を示すフローチャートである。

【図４】同上方法例のシーケンスチャートである。

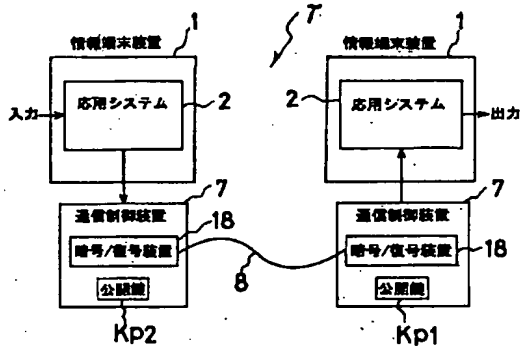
【図５】従来例の暗号通信システム装置の構成ブロック図である。

【図６】他の従来例の暗号通信システム装置の構成ブロック図である。

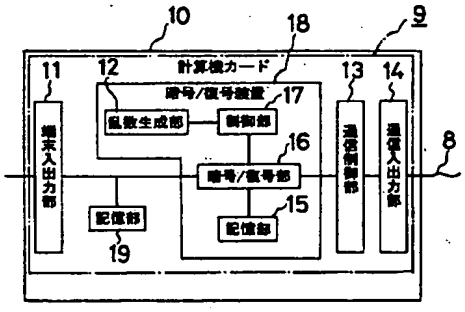
【符号の説明】

α，β，γ…暗号通信システム装置
１…情報端末装置
２…応用システム
３，１８…暗号／復号装置
４，６…暗号鍵
５…外部記憶装置
７…通信制御装置
８…通信路
９…暗号通信装置
１０…計算機カード
１１…端末入出力部
１２…乱数生成部
１３…通信制御部
１４…通信入出力部
１５，１９…記憶部
１６…暗号／復号部
１７…制御部
１８…暗号／復号装置
Ｋｐ１，Ｋｐ２…公開鍵
Ｋｅ１，Ｋｅ２…暗号鍵
Ｍ１，Ｍ２…送・受信データ
Ｋｅ１［Ｍ１］，Ｋｅ２［Ｍ２］…暗号化データ
Ｋｐ１［Ｋｅ２］，Ｋｐ２［Ｋｅ１］…保護暗号鍵

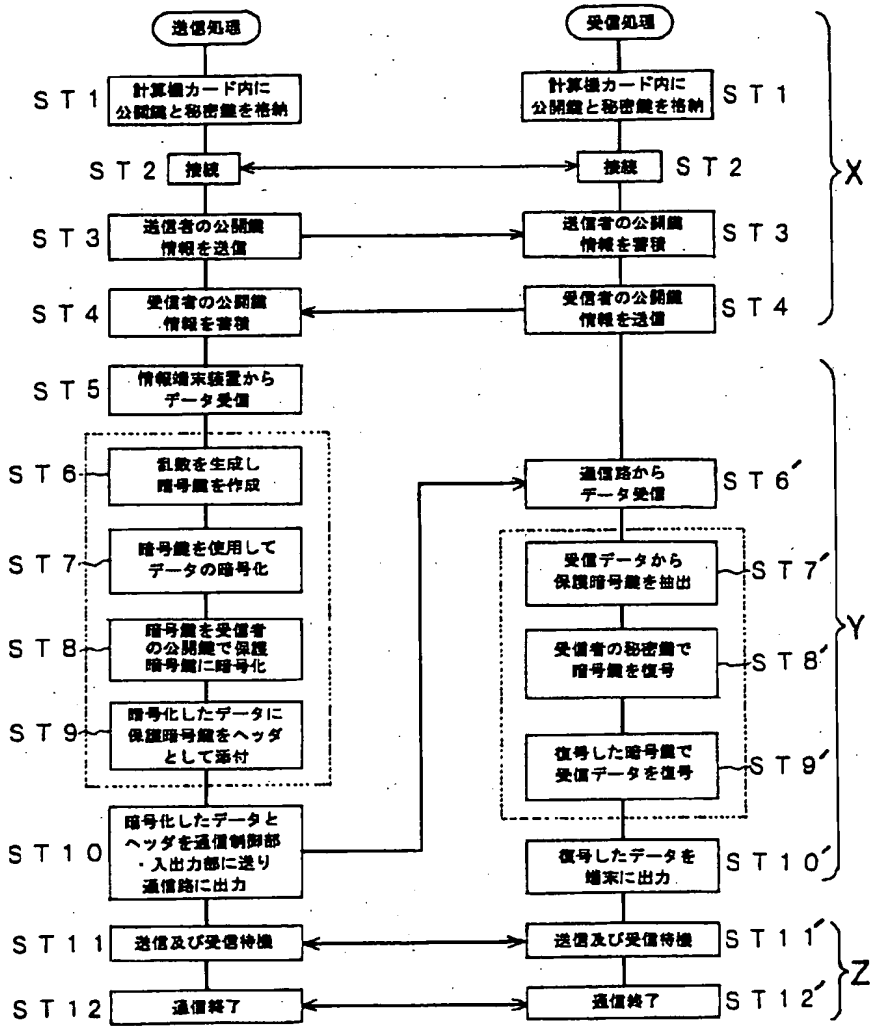
【図１】



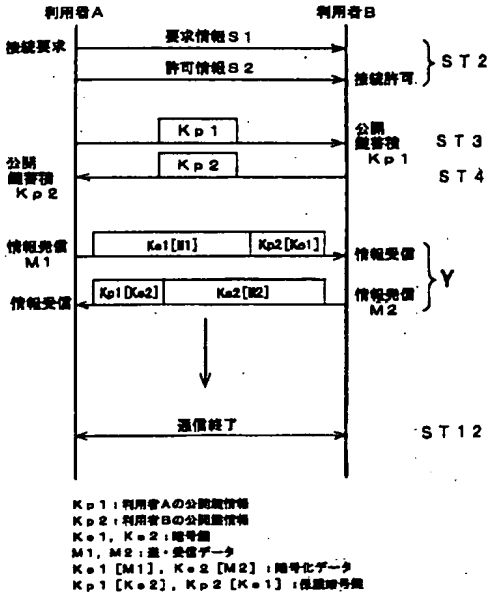
【図２】



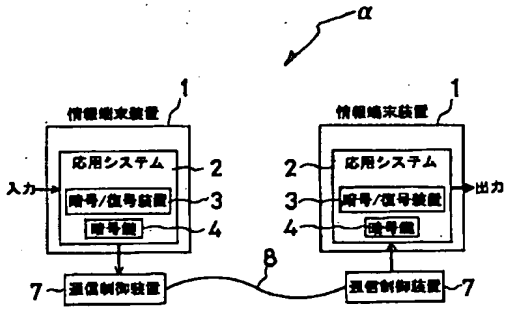
【図３】


送信処理
受信処理
ＳＴ１
計算機カード内に公開鍵と秘密鍵を格納
計算機カード内に公開鍵と秘密鍵を格納
ＳＴ１
ＳＴ２
接続
接続
ＳＴ２
X
ＳＴ３
送信者の公開鍵情報を送信
送信者の公開鍵情報を蓄積
ＳＴ３
ＳＴ４
受信者の公開鍵情報を蓄積
受信者の公開鍵情報を送信
ＳＴ４
ＳＴ５
情報端末装置からデータ受信
ＳＴ６
乱数を生成し暗号鍵を作成
通信路からデータ受信
ＳＴ６′
ＳＴ７
暗号鍵を使用してデータの暗号化
受信データから保護暗号鍵を抽出
ＳＴ７′
ＳＴ８
暗号鍵を受信者の公開鍵で保護暗号鍵に暗号化
受信者の秘密鍵で暗号鍵を復号
ＳＴ８′
Y
ＳＴ９
暗号化したデータに保護暗号鍵をヘッダとして添付
復号した暗号鍵で受信データを復号
ＳＴ９′
ＳＴ１０
暗号化したデータとヘッダを通信制御部・入出力部に送り通信路に出力
復号したデータを端末に出力
ＳＴ１０′
ＳＴ１１
送信及び受信待機
送信及び受信待機
ＳＴ１１′
Z
ＳＴ１２
通信終了
通信終了
ＳＴ１２′

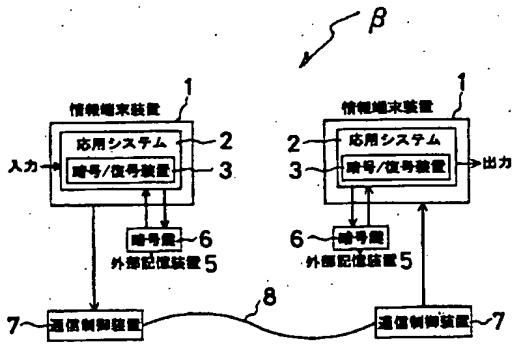
【図４】


利用者A
利用者B
接続要求
要求情報S1
許可情報S2
接続許可
ST2
Kp1
公開鍵登録
Kp1
ST3
公開鍵登録
Kp2
Kp2
ST4
情報発信
M1
Ke1[M1]
Kp2[Ke1]
情報受信
情報受信
Kp1[Ke2]
Ke2[M2]
情報発信
M2
Y
通信終了
ST12
Kp1：利用者Aの公開鍵情報
Kp2：利用者Bの公開鍵情報
Ke1，Ke2：暗号鍵
M1，M2：送・受信データ
Ke1［M1］，Ke2［M2］：暗号化データ
Kp1［Ke2］，Kp2［Ke1］：保護暗号鍵

【図５】


α
情報端末装置
1
応用システム
2
暗号/復号装置
3
暗号鍵
4
入力
出力
7
通信制御装置
8

【図６】


β
情報端末装置
1
応用システム
2
暗号/復号装置
3
入力
出力
暗号鍵
6
外部記憶装置
5
7
通信制御装置
8